CLAIMS

1. A method comprising:

achieving agreement among n participating network devices in an asynchronous network for deciding on a common value (v) being validated by a justification (p) together satisfying a predetermined predicate (Q), a agreement arising out of a series of messages being sent and received by each participating network device with up to a number t of faulty devices, each participating network device performing the following steps:

i) broadcasting to the participating network devices an echo message comprising a proposed value (w) and a proposed justification (π) by using verifiable and consistent broadcast;

ii) receiving n-t echo messages comprising candidate values (w_1, w_2, w_3) and candidate justifications (π_1, π_2, π_3) satisfying the predicate (Q), and

repeating the following steps 1) to 3) for each participating network device as a candidate device represented by a candidate device identifier (a) according to an order:

1) broadcasting to all participating network devices a vote message comprising the candidate device identifier (a), and either a first agree-value (Y) together with the candidate value (w_a) and the candidate justification (π_a), or a second agree-value (N),

2) receiving vote messages and counting up to n-t vote messages including the second agree-value (N) or the first agree-value (Y), the candidate value (w_a), and the candidate justifications (π_a) satisfying the predicate (Q),

3) performing a Byzantine agreement to determine whether the candidate device has sent the candidate value (w_a) and the candidate justification (π_a) satisfying the predicate (Q),

iii) in response to the result of the Byzantine agreement, deciding the common value (v) proposed as the candidate value (w) and the justification (p) proposed as the candidate justification (π) of an agreed candidate device.

2. Method according to claim 1, whereby step ii) further comprises
- broadcasting a commit message comprising sender identities of received echo messages,
- receiving commit messages,
- selecting randomly the order of the candidate device by opening at least one cryptographic common coin,
- and whereby in step 2) the vote messages are counted which are consistent with the received commit messages.

3 Method according to claim 2, whereby the step of opening at least one cryptographic common coin comprises using a distributed coin-tossing protocol.

4. Method according to claim 1, whereby in step i) the verifiable and consistent broadcast comprises a certified delivery of the broadcasted echo message within a sent message and reaching agreement on the content of the broadcasted echo message.

5. Method according to claim 1, whereby in step i) the verifiable and consistent broadcast comprises exchanging signed messages between the participating network devices .

6. Method according to claim 1, whereby in step i) the verifiable and consistent broadcast comprises using threshold signatures.

7. Method according to claim 1, whereby steps 1) and 2) in step ii) comprise broadcasting the candidate value (w_a) and the candidate justification (π_a) upon a request.

8. Method according to claim 1, whereby in step ii) the participating network devices are voting on several candidate devices simultaneously.

9. A method for reliably broadcasting messages in an order within an asynchronous network comprising *n* participating network devices and tolerating a number *t* of less than *n*/3 faulty participating network devices, each participating network device storing a queue (*q*) and a log (*d*), the method operating in rounds, each round comprising the following steps:

i) responsive to a message broadcast request comprising a message value (*m*) performing the step of:
appending the message value (*m*) to the queue (*q*) unless the log (*d*) or the queue (*q*) comprises the message value (*m*),

ii) deriving a signature (σ) on the queue (*q*),

iii) broadcasting to all participating network devices a queue message comprising the queue (*q*) and the signature (σ),

iv) receiving a number *c* of at least *t*+1 queue messages comprising *c* proposed queues and proposed signatures ,

v) storing the proposed queues in a queue vector (QV) and the proposed signatures in a signature vector (SV),

vi) proposing the queue vector (QV) for Byzantine agreement validated by the signature vector (SV) and performing a method for achieving agreement on a common value being validated by a justification (*p*) together satisfying a predetermined predicate (*Q*) by validating the queue vector (QV) and the signature vector (SV) through a determined predicate (Q) asserting that the

signature vector (SV) comprises *c* valid signature entries of distinct participating network devices (A, B, C) on entries of the queue vector (QV),

vii) preparing in response to the result of the Byzantine agreement an ordered list (L) of unique message values out of the entries of the decided queue vector (DQV)

viii) accepting the unique message values in the ordered list (L) in the sequence of the ordered list (L),

ix) appending the accepted unique message values to the log (*d*).

10. Method according to claim 9, whereby step of performing a method for achieving agreement on a common value comprises:

achieving agreement among *n* participating network devices in an asynchronous network for deciding on a common value (*v*) being validated by a justification (*p*) together satisfying a predetermined predicate (*Q*), the agreement arising out of a series of messages being sent and received by each participating network device with up to a number *t* of faulty devices, each participating network device performing the following steps:

i) broadcasting to the participating network devices an echo message comprising a proposed value (*w*) and a proposed justification (π) by using verifiable and consistent broadcast;

ii) receiving *n-t* echo messages comprising candidate values (w_1, w_2, w_3) and candidate justifications (π_1, π_2, π_3) satisfying the predicate (*Q*), and

repeating the following steps 1) to 3) for each participating network device as a candidate device represented by a candidate device identifier (a) according to an order:

2) broadcasting to all participating network devices a vote message comprising the candidate device identifier (a), and either a first agree-value (Y) together with the candidate value (w_a) and the candidate justification (π_a), or a second agree-value (N),

2) receiving vote messages and counting up to n-t vote messages including the second agree-value (N) or the first agree-value (Y), the candidate value (w_a), and the candidate justifications (π_a) satisfying the predicate (Q),

3) performing a Byzantine agreement to determine whether the candidate device has sent the candidate value (w_a) and the candidate justification (π_a) satisfying the predicate (Q),

iii) in response to the result of the Byzantine agreement, deciding a common value (v) proposed as the candidate value (w) and the justification (p) proposed as the candidate justification (π) of an agreed candidate device.

11. Method according to claim 9, whereby step iv) further comprises appending an unknown message value found in a received queue message to the queue (q) unless the log (d) or the queue (q) comprises the unknown message value.

12. Method according to claim 1, whereby the number t of faulty devices is extended to a set T of sets comprising participating network devices.

13. Method according to claim 12, whereby the participating network devices show hybrid failures (BF, CF, LF) reflecting a different structure of the set T or different thresholds t_i, with $i = 1, 2, \ldots l$.

14. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing achievement of

agreement, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

15. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing reliable broadcasting of messages, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 9.

16. Method according to claim 9, whereby the number t of faulty devices is extended to a set T of sets comprising participating network devices.

17. Method according to claim 16, whereby the participating network devices show hybrid failures (BF, CF, LF) reflecting a different structure of the set T or different thresholds t_i, with $i = 1, 2, \ldots l$.

18. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for causing achievement of agreement, said method steps comprising the steps of claim 1.

19. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for causing reliable broadcasting of messages, said method steps comprising the steps of claim 9.

20. A system comprising:

means for achieving agreement among n participating network devices in an asynchronous network for deciding on a common value (v) being validated by a justification (p) together satisfying a predetermined predicate (Q), the agreement arising out of a series of messages being sent and received by each participating network device with up to a number t of faulty devices, each participating network device including:

i) means for broadcasting to the participating network devices an echo message comprising a proposed value (w) and a proposed justification (π) by using verifiable and consistent broadcast;

ii) means for receiving n-t echo messages comprising candidate values (w_1, w_2, w_3) and candidate justifications (π_1, π_2, π_3) satisfying the predicate (Q), and

repeating the following steps 1) to 3) for each participating network device as a candidate device represented by a candidate device identifier (a) according to an order:

3) means for broadcasting to all participating network devices a vote message comprising the candidate device identifier (a), and either a first agree-value (Y) together with the candidate value (w_a) and the candidate justification (π_a), or a second agree-value (N),

2) means for receiving vote messages and counting up to n-t vote messages including the second agree-value (N) or the first agree-value (Y), the candidate value (w_a), and the candidate justifications (π_a) satisfying the predicate (Q),

3) means for performing a Byzantine agreement to determine whether the candidate device has sent the candidate value (w_a) and the candidate justification (π_a) satisfying the predicate (Q),

iii) means for deciding in response to the result of the Byzantine agreement, the common value (v) proposed as the candidate value (w) and the justification (p) proposed as the candidate justification (π) of an agreed candidate device.

21. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing achievement of agreement, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 20.